Password in Active Directory attributes

Inb order to search through users or objects you need to

Interesting attributes to search for, remember these can be for either computer or a user.

```
 comment
description
UserPassword
UnixUserPassword
unicodePwd
msSFU30Password
```

Other interesting might be

```
 adminDescription
dBCSPwd
lmpwdHistory
nTPwdHistory
supplementalCredentials
```

Using PowerView

```
 Get-DomainUser -Domain evilcorp.local -Properties samaccountname,comment,description,userpassword,unixuserpassword,unicodepwd,mssfu3
```

Using ldap query

```
 ldapsearch -h evilcorp.local  -w SecretPassword  -b "dc=evilcorp,dc=local" -D "cn=Philip L,cn=users,dc=evilcorp,dc=local" "(|(userPa
```

These will generate a lot of results, and you will have to go through the result one by way, or just grep for relevant words. If the LDAP server has a maxsize of results to display, it will cap the response at that size. To get around that, and to not make mega-queries, your can set a size-limit, and then be promped to receive more.

If the response contains åäö the result is base64-encoded.

```
 ldapsearch -E pr=500/prompt -h evilcorp.local  -w SecretPassword  -b "dc=evilcorp,dc=local" -D "cn=Philip L,cn=users,dc=evilcorp,dc=

grep -i 'pwd\|passw\|lösen\|losen\|somma\|vinter\|'
```

Or you can perform the search in the LDAP query itself:

```
 ldapsearch -h evilcorp.local  -w SecretPassword  -b "dc=evilcorp,dc=local" -D "cn=Philip L,cn=users,dc=evilcorp,dc=local" "(|(descri
```

Debugging problems

If you receive this error it means that you are not allowed to authenticate to the LDAP server from your HOST.

```
additional info: 80090308: LdapErr: DSID-0C09042A, comment: AcceptSecurityContext error, data 531, v3839
```

On your AD users there exists an attribute called `userWorkstations`, this attribute specified from which workstations you are allowed to authenticate to the LDAP server. Since your linux-machines hostname is not among those specified in the `userWorkstations` attribute you are not allowed.

A possible workaround, that I have not tested but might work, is to change the hostname to a hostname that is specified in `userWorkstations` attribute of the user. This presents a catch22, because you need LDAP access to know which `userWorksations` are allowed.

Using Bloodhound and bash

```
echo "match (a) return a.description;"  | /usr/share/neo4j/bin/cypher-shell -u neo4j -p <creds> --format plain  | sort -u
```

Using ActiveDirectory module

```
 # This will only search for a specific OU
Get-ADUser -Filter * -SearchBase "OU=Users OU,DC=hackdomain,DC=local" -Properties comment

# This will search for the whole domain
Get-ADUser -Filter * -SearchBase "DC=hackdomain,DC=local" -Properties comment
```